

CLAIMS

What is claimed is:

- 1 1. A method for monitoring intrusion activity utilizing a plurality of firewalls,  
2 comprising:
  - 3 (a) establishing network communications with a plurality of computers with  
4 firewalls over a network, wherein the firewalls are adapted for collecting  
5 information relating to intrusion activity;
  - 6 (b) collecting the information from the firewalls of the computers utilizing the  
7 network; and
  - 8 (c) transmitting a response to the firewalls of the computers utilizing the  
9 network;
  - 10 (d) wherein the firewalls are adapted for preventing the intrusion activity  
11 utilizing the response.
- 1 2. The method as recited in claim 1, and further comprising heuristically  
2 analyzing the information to ascertain intrusion activity.
- 1 3. The method as recited in claim 1, and further comprising generating rules for  
2 preventing the intrusion activity utilizing the firewalls.
- 1 4. The method as recited in claim 3, wherein the response includes the rules.
- 1 5. The method as recited in claim 1, wherein the information is collected by the  
2 firewalls automatically.
- 1 6. The method as recited in claim 5, wherein the information is collected by the  
2 firewalls periodically.

1 7. The method as recited in claim 1, wherein the information is transmitted  
2 utilizing an HTTP protocol.

1 8. A system for monitoring intrusion activity utilizing a plurality of firewalls,  
2 comprising:

3 (a) logic for establishing network communications with a plurality of computers  
4 with firewalls over a network, wherein the firewalls are adapted for  
5 collecting information relating to intrusion activity;

6 (b) logic for collecting the information from the firewalls of the computers  
7 utilizing the network; and

8 (c) logic for transmitting a response to the firewalls of the computers utilizing  
9 the network;

10 (d) wherein the firewalls are adapted for preventing the intrusion activity  
11 utilizing the response.

1 9. A computer program product for monitoring intrusion activity utilizing a  
2 plurality of firewalls, comprising:

3 (a) computer code for establishing network communications with a plurality of  
4 computers with firewalls over a network, wherein the firewalls are adapted  
5 for collecting information relating to intrusion activity;

6 (b) computer code for collecting the information from the firewalls of the  
7 computers utilizing the network; and

8 (c) computer code for transmitting a response to the firewalls of the computers  
9 utilizing the network;

10 (d) wherein the firewalls are adapted for preventing the intrusion activity  
11 utilizing the response.

1 10. A method for reporting intrusion activity utilizing a plurality of firewalls,  
2 comprising:

- 3 (a) establishing network communications with a plurality of computers with  
4 firewalls over a network, wherein the firewalls are adapted for collecting  
5 information relating to intrusion activity;
- 6 (b) collecting the information from the firewalls of the computers utilizing the  
7 network;
- 8 (c) analyzing the information to ascertain intrusion activity;
- 9 (d) identifying a source of the ascertained intrusion activity; and
- 10 (e) notifying the source of the ascertained intrusion activity.

1 11. The method as recited in claim 10, wherein the information is heuristically  
2 analyzed.

1 12. The method as recited in claim 10, wherein the identification of the source  
2 includes identifying an Internet Protocol (IP) address associated with at least  
3 one source of the intrusion activity.

1 13. The method as recited in claim 12, wherein the identification of the source  
2 further includes looking up an electronic-mail address based on the IP  
3 address.

1 14. The method as recited in claim 10, wherein the notification includes an  
2 electronic mail.

1 15. The method as recited in claim 10, wherein the notification includes a  
2 summary of the intrusion activity.

1 16. The method as recited in claim 10, and further comprising determining  
2 whether a response to the notification is received.

1 17. The method as recited in claim 16, wherein if it is determined that the  
2 response to the notification is not received, reporting the source of the  
3 intrusion activity to a central intrusion activity watch service.

1 18. The method as recited in claim 17, wherein the central intrusion activity  
2 watch service notifies the public of the source of the intrusion activity via a  
3 web interface.

1 19. A system for reporting intrusion activity utilizing a plurality of firewalls,  
2 comprising:  
3 (a) logic for establishing network communications with a plurality of computers  
4 with firewalls over a network, wherein the firewalls are adapted for  
5 collecting information relating to intrusion activity;  
6 (b) logic for collecting the information from the firewalls of the computers  
7 utilizing the network;  
8 (c) logic for analyzing the information to ascertain intrusion activity;  
9 (d) logic for identifying a source of the ascertained intrusion activity; and  
10 (e) logic for notifying the source of the ascertained intrusion activity.

1 20. A computer program product for reporting intrusion activity utilizing a  
2 plurality of firewalls, comprising:  
3 (a) computer code for establishing network communications with a plurality of  
4 computers with firewalls over a network, wherein the firewalls are adapted  
5 for collecting information relating to intrusion activity;  
6 (b) computer code for collecting the information from the firewalls of the  
7 computers utilizing the network;  
8 (c) computer code for analyzing the information to ascertain intrusion activity;  
9 (d) computer code for identifying a source of the ascertained intrusion activity;  
10 and  
11 (e) computer code for notifying the source of the ascertained intrusion activity.

- 1 21. A method for monitoring intrusion activity utilizing a firewall, comprising:  
2 (a) collecting information relating to intrusion activity utilizing a firewall  
3 associated with a computer;  
4 (b) transmitting the information from the firewall associated with the computer  
5 to a central server utilizing the network;  
6 (c) receiving a response from the central server utilizing the network;  
7 (d) wherein the firewall is adapted for preventing the intrusion activity utilizing  
8 the response.

- 1 22. A method for monitoring intrusion activity utilizing a plurality of firewalls,  
2 comprising:  
3 (a) establishing network communications with a plurality of computers with  
4 firewalls over a network, wherein the firewalls are adapted for collecting  
5 information relating to intrusion activity;  
6 (b) collecting the information from the firewalls of the computers utilizing the  
7 network;  
8 (c) heuristically analyzing the information to ascertain intrusion activity;  
9 (d) generating rules for preventing the intrusion activity utilizing the firewalls  
10 based on the heuristic analysis;  
11 (e) transmitting the rules to the firewalls of the computers utilizing the network,  
12 wherein the firewalls are adapted for preventing the intrusion activity  
13 utilizing the rules;  
14 (f) identifying an Internet Protocol (IP) address associated with at least one  
15 source of the intrusion activity;  
16 (g) looking up an electronic-mail address based on the IP address;  
17 (h) generating a summary of the information relating to the intrusion activity  
18 associated with the source;  
19 (i) transmitting the summary to the electronic-mail address in the form of  
20 electronic-mail;  
21 (j) determining whether a response to the electronic-mail is received; and

- 22 (k) if it is determined that the response to the electronic-mail is not received,  
23 reporting the source of the intrusion activity to a central intrusion activity  
24 watch service, wherein the central intrusion activity watch service notifies  
25 the public of the source of the intrusion activity via a web interface.

2007-03-20 10:00:00